

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with "kegreen874@gmail.com"
that is stored at premises controlled by Google

Case No. 22MJ

121

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. §§ 1341, 1343
1349, 1956, 1957

Offense Description
Mail fraud; wire fraud; attempt and conspiracy; money laundering; and engaging in monetary transactions in property derived from specific unlawful activity

The application is based on these facts:

See affidavit of Special Agent Phillip W. Spainhour

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

15/ Phillip Spainhour
Applicant's signature

Phillip W. Spainhour, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone after e-mailing doubts (specify reliable electronic means).

Date:

03/14/22

City and state: Greensboro, NC

Judge's signature

Honorable L. Patrick Auld

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Google account “kegreen874@gmail.com” that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

I. Information to be disclosed by Google LLC (the “Target Provider”).

To the extent that the information described in Attachment A is within the possession, custody, or control of Google LLC (“Google”), regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that have been deleted but are still available to Google, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A, from January 1, 2017 to the present:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of Title 18, United States Code, Sections 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Attempt and Conspiracy), 1956 (Money Laundering), and 1957 (Engaging in Monetary Transaction in Property Derived from Specific Unlawful Activity) involving the SUBJECT ACCOUNT from January 1, 2017 to present, specifically, identified in Attachment A, information pertaining to the following matters:

- a. Evidence of the identities and locations of the individuals with access to the SUBJECT ACCOUNT;
- b. Documents or communications between and among the user of the SUBJECT ACCOUNT and any individual purporting to be "Lesley;"
- c. Documents or communications between and among the user of the SUBJECT ACCOUNT and any individuals referencing the individuals G.M. and J.F. as described in the supporting affidavit;
- d. Documents or communications between and among any individuals referencing money wires or transfers and bank accounts and/or deposits; and
- e. Evidence indicating how and when, and by whom, the SUBJECT ACCOUNT was accessed and used for any of the items authorized for seizure by the warrant, including records and information that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be

conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Google is hereby ordered to disclose the above information to the government within fourteen days of service of this warrant.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
GOOGLE ACCOUNT
"KEGREEN874@GMAIL.COM" THAT IS
STORED AT PREMISES CONTROLLED BY
GOOGLE LLC

Case No. 1:22mj0121

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT FOR

I, Phillip W. Spainhour, Special Agent of the Federal Bureau of Investigation (FBI),
being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI). I am an "investigative or law enforcement officer of the United States," within the meaning of Section 2510(7) of Title 18, United States Code, that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Section 2516, Title 18, United States Code.

2. I have been a SA with the FBI for nearly 14 years. I am currently assigned to the Charlotte Division at the Greensboro Resident Agency, and focus on investigations involving Public Corruption, Civil Rights, and White Collar Crime. Prior to the FBI, I served over ten years as a Detective and Deputy Sheriff with the Forsyth County Sheriff's Office, in Winston-Salem, North Carolina. I have completed hundreds of hours of training in numerous areas of law enforcement investigations and techniques, including but not limited to the following: Basic Law Enforcement Training through the State of North Carolina; Specialized training through the North Carolina Justice Academy; FBI New Agents Training in Quantico, Virginia; and Specialized Federal Law Enforcement training involving White Collar Crime, Public Corruption,

Health Care Fraud, Evidence Response Team (ERT), Organized Crime Drug Enforcement Task Force (OCDETF), Money Laundering, Asset Forfeiture, Counterintelligence, and Domestic and International Terrorism. I have participated in and conducted investigations of illegal activity involving violent crime, drug and firearms trafficking, gang activity, fraud, money laundering, public corruption, civil rights, white collar crime, domestic and international terrorism, and other violations against the United States. Those investigations have led to the indictments, arrests, and convictions of numerous individuals for various state and federal criminal violations.

3. Affiant makes this affidavit in support of an application for a search warrant for information associated with Google Account—kegreen874@gmail.com—the “SUBJECT ACCOUNT”) that is stored at premises owned, maintained, controlled, or operated by Google LLC (“Google”), an electronic communications service provider, headquartered at 1600 Amphitheater Parkway, Mountain View, California.

4. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Google to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

5. Based on the facts as set forth, the affiant submits there is probable cause to believe that Kenneth Green (Green), user of the SUBJECT ACCOUNT, and others have committed violations of Title 18, United States Code, Sections 1341 (Mail Fraud), 1343 (Wire Fraud), 1349 (Attempt and Conspiracy), 1956 (Money Laundering), and 1957 (Engaging in Monetary Transaction in Property Derived from Specific Unlawful Activity) (collectively, the

“SUBJECT OFFENSES”); between approximately January 1, 2017 and February 28, 2020. As described below, Green is the user of the SUBJECT ACCOUNT and there is probable cause to believe evidence of the SUBJECT OFFENSES is contained in the SUBJECT ACCOUNT that is stored at premises controlled by Google, LLC.

6. This affidavit is based on my personal investigation and investigation by others. The facts contained herein have been obtained by interviewing witnesses and examining documents obtained in the course of the investigation, as well as through other means. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. §§ 2711, 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

FACTS IN SUPPORT OF PROBABLE CAUSE

8. On or about May 28, 2019, the FBI, Charlotte Division, Greensboro Resident Agency received information from K.Y. through the FBI’s National Threat Operation Center (NTOC) indicating her father, J.F., was a victim of a romance and gold inheritance investment fraud scheme.

9. K.Y.’s uncle, and J.F.’s brother-in-law, G.M. relocated from Missouri to North Carolina in approximately October of 2016, following J.F.’s wife’s, D.F.’s, death.

10. During this same time frame G.M. began an online and telephonic friendship and romance with a person he believed was named Lesley Hobson, aka: Lesley Hobson Green

(Lesley). G.M. believed Lesley was a white female who was born in 1983. G.M. met Lesley through the online dating website ChristianMingle.com. Lesley convinced G.M. she had inherited 16 gold bars that were put into a trust following the death of her father and brother in a car accident in Germany when she was a child.

11. G.M. believed Lesley lived in New York with her mother, Mercy Green (Mercy) and her uncle, Kenneth Green (Kenneth), aka: Uncle Kenneth/Kenny. Lesley convinced G.M and J.F. through G.M. to send her and others money on her behalf to pay the taxes and fees associated with collecting the gold inheritance.

12. During voluntary interviews with FBI special agents on September 4, 2020 and September 17, 2020, G.M. said Lesley took care of Mercy because she suffered from an orthopedic condition and Kenneth because he had COPD. According to G.M., he met Lesley, Mercy, and Kenneth in person during two trips he made to New York in 2018 and 2019. G.M. described Kenneth as a white male in his late 50's to early 60's, with a medium build, approximately 5 foot, 9 inches tall, 175 pounds, with full grayish colored hair and a German accent. G.M. communicated with Lesley at the email address bemabae22@gmail.com and telephone number (934) 223-2695.¹ G.M. said Lesley also had a German accent. A special agent showed G.M. pictures of a woman with brown hair that were recovered from records associated with email address bemabae22@gmail.com. G.M confirmed the pictures were of who he believed to be Lesley.

¹ The FBI received communication and image contents from the email address bemabae22@gmail.com through a search warrant obtained by the Forsyth County Sheriff's Office, in Winston-Salem, NC.

13. A review of the search warrant materials for bemabae22@gmail.com showed the last Internet Protocol (IP) address used to access the email account on June 10, 2019, resolved to Accra, Ghana.

14. Affiant attempted to identify the subscriber/user of telephone number (934) 223-2695 through the service of legal process on Onvoy, LLC (dba: Inteliquent), who provided a response stating the number was assigned to Textnow.com. Affiant served legal process on Textnow.com attempting to identify the subscriber/user between the dates January 1, 2017 through March 12, 2021, but was unable to do so because the results only covered the dates April 6, 2020 through October 1, 2020. The dates for offense in this investigation ranged from March of 2017 through April of 2019. The information provided by Textnow.com did not include full names, dates of birth, addresses or payment information and was therefore not sufficient to fully identify the actual subscriber/user by true name. The IP addresses associated with the various subscriber/user names provided by Textnow.com resolved to India, Indonesia, and Iran.

15. J.F. and D.F. had accumulated between two and three million dollars in their retirement investment accounts prior to D.F.'s death. J.F. lost approximately \$1,170,240 as a result of his victimization by the fraud scheme involving Lesley, G.M., and others as yet unknown.

16. The FBI received various bank records in connection with this investigation. Analysis of those records showed that unidentified subjects directed G.M. and J.F. to deposit and wire transfer money into different bank accounts at various banks throughout the United States. The accounts were in the names of unknown individuals (likely people serving as "money mules"). G.M. and J.F. received emails from Lesley's bemabae22@gmail.com email account and other unknown email accounts including secbukbank@accountant.com that provided wire

instructions in the form of account holder names, bank names, account numbers, routing numbers, bank swift codes, and physical addresses. G.M and J.F. were instructed to send specific amounts of money as directed in emails for specific purposes such as taxes, fees, and other costs associated with receiving funds from gold inheritances.

17. Once J.F. and G.M. funds were deposited into the bank accounts, the funds were moved out using different methods, including the following: transfers to businesses and individuals, transfers into cryptocurrency, and the purchase of vehicles shipped to Ghana and Nigeria. Several of the individuals whose bank accounts were used to receive the money from G.M. and J.M. had immigrated to the United States from either Ghana or Nigeria.

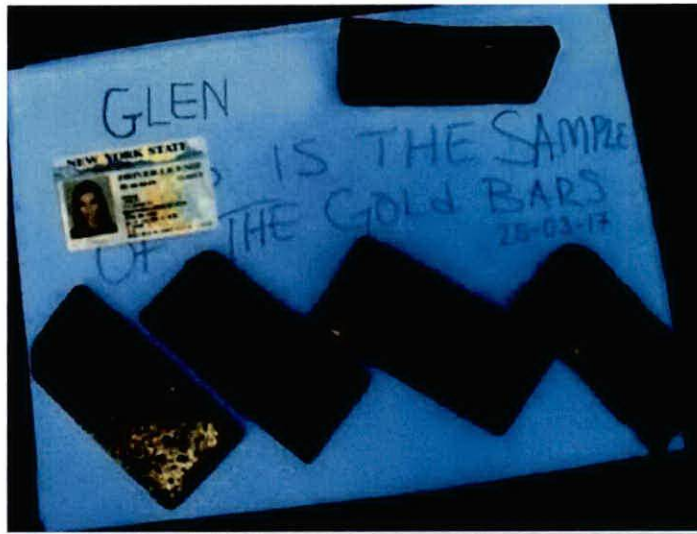
Identification of Kenneth Green

18. At Lesley's and others' direction, through emails that sometimes included secbukbank@accountant.com, telephone calls, and text messages, G.M. and J.F. deposited and wire transferred approximately \$457,756 into bank accounts controlled by Green. The investigation identified Green as Kenneth Green, a black male, born in 1970, with an address at an apartment complex in Staten Island, New York. Agents also identified a former address associated with Green in North Bellmore, New York.

19. During an interview with G.M. on September 4, 2020, special agents showed him a photograph of Green for identification purposes. G.M. did not recognize Green.

20. During an interview with G.M. on September 17, 2020, he said Lesley sent him a photo of several gold bars on a piece of paper with writing that included his name and her New York driver's license. G.M. provided a copy of that picture, which is reproduced as Image 1 below:

Image 1



The address on the license in Image 1 is Green's former address in North Bellmore, New York. During an interview with G.M., agents advised him the driver's license number and address used in the photo belonged to the identified Green, not Lesley. G.M. appeared shocked to learn the real Green was an unemployed, adult, black male, who lived with his mother and not the previously described man he'd met as Uncle Kenneth/Kenny during his New York visit to see Lesley.

21. G.M. confirmed he mailed cards, flowers, nightwear, and other items to Lesley at the two above-mentioned addresses associated with Green. Lesley sent G.M. photos of the items he'd sent, as confirmation that she had received them. Two of such images are reproduced below.

Image 2

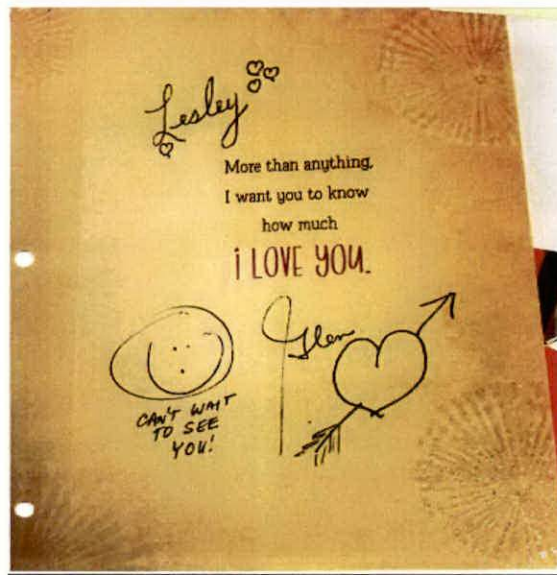
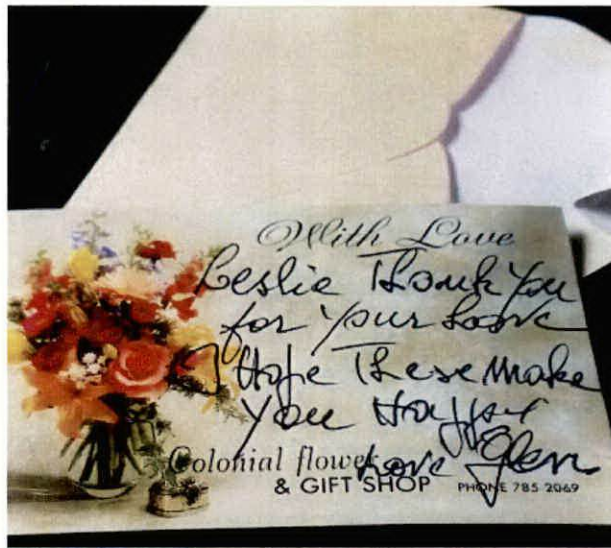


Image 3



Agents advised G.M. these addresses were the former and current residences of the identified Green, not Lesley. Agents also showed G.M. a photograph of the apartment complex in Staten Island (i.e., Green's current residence). G.M. said the picture was consistent with his recollection of Lesley's apartment complex where he stayed with her during his 2018 visit.

22. On January 6, 2021, special agents interviewed the apartment manager, D.S. D.S. was shown multiple photographs of Lesley and provided with the descriptions of Mercy and Kenneth that G.M. gave the FBI. D.S. did not recognize the photographs or descriptions as matching any former or current residents of the apartment complex.

23. On February 20, 2020, special agents interviewed Green at his apartment in Staten Island where he lived with his mother, J.U.F. Green admitted having bank accounts with Wells Fargo, Citibank, Chase, Santander, and Capital One during the time frame in question. Green initially lied to agents stating the money he received from J.F. was because of family issues involving J.F. Green later admitted he had never met J.F. and did not remember why he had received the money. Green admitted receiving hundreds of thousands of dollars in funds from G.M and J.F. into the various bank accounts he controlled. Green further admitted he sent the majority of those funds to individuals located in Ghana at the direction of Lesley.

24. According to Green, he began a friendship/romantic relationship with Lesley after receiving an unsolicited email from her in 2017. Green communicated with Lesley using his email address kegreen874@gmail.com—i.e., the SUBJECT ACCOUNT. Green may have also communicated with Lesley using the following email accounts: kegreen874@yahoo.com, kegreen31@gmail.com and kegreen31@yahoo.com.

25. Special agents showed Green a copy of the fictitious New York driver's license Lesley sent to G.M. so as to confirm her identity/legitimacy. Green confirmed the address and license number shown were his but said he did not know the woman depicted in the driver's license photo. Green did not deny providing his driver's license information to Lesley.

26. Green told agents he provided his bank account information to Lesley to allow her to have money deposited directly into accounts he controlled. Lesley gave Green instructions

by email of what funds were being wired or deposited into his accounts and where to send those funds after he had received them. Green used his Wells Fargo bank account for this purpose until it was closed by Wells Fargo.

27. Green said he provided Lesley with the password to his email account kegreen874@gmail.com (the SUBJECT ACCOUNT) so she could independently verify when he received emails from Wells Fargo notifying him that an incoming wire transfer had been received into his account. Green could not recall whether or not he had given Lesley access/passwords for any of his other email accounts, but said it was possible.

28. During the interview with Green, agents discussed with him a series of transactions in which he received money from either G.M. or J.F. After receiving the money, Green sent most of it by wire transfer to Ghana. Green also withdrew some of the money in cash and transferred it using Western Union or Money Gram. Green said he sent large amounts through bank wire transfers and smaller amounts through money remitter services so they would reach Lesley faster. According to Green, due to the amount, frequency, and destination of the smaller wire transfers he was sending, his name was flagged by Western Union and Money Gram. Green lied to Western Union and Money Gram employees telling them he had family members in Ghana so they would allow him to continue sending money, which they did.

29. Green said all of his communication with Lesley was by email and he did not talk with her over the phone, social media, or video calls.

30. Green also admitted engaging in the re-shipping of packages at Lesley's request. Green claimed he sent packages containing Apple iPhones to locations in Ghana at addresses Lesley provided him at email address kegreen874@gmail.com (the SUBJECT ACCOUNT).

31. During Green's interview, special agents admonished him with the Money Mule letter warnings verbally and advised they would send him an official letter at a later date. On February 24, 2020, at 4:17pm, affiant sent Green a Money Mule letter by email and requested that he read, sign, and return the letter by mail. On February 24, 2020, at 6:49pm, Green responded to affiant's email and stated: "Thank you, will do." However, Green never returned a signed Money Mule letter to the FBI.

32. During the interview, Green voluntarily provided agents with written consent for the search of his gmail.com and yahoo.com email accounts on two FD-26 consent to search forms. Affiant served Google/Gmail and Yahoo/Oath with copies of the applicable FD-26 consent to search forms through their Law Enforcement Portals. On March 16, 2020, Google notified the affiant it did not accept consent requests, but that the account holder (Green) could use the Google Takeout service to obtain content directly from his email account to law enforcement. Affiant forwarded this information to Green by email and requested a copy of the email content for all of his Google and Yahoo email accounts. Green never responded to the affiant's request or provided any account content information to the FBI.

33. On January 6, 2021, FBI special agents interviewed J.U.F., Green's mother, at their apartment in Staten Island, New York. Agents showed J.U.F. multiple photographs of Lesley and provided with the descriptions of Mercy and Kenneth that G.M. gave the FBI. J.U.F. did not recognize the female depicted in the photographs and did not know anyone in the apartment complex that matched the descriptions of Mercy or Kenneth.

34. J.U.F. remembered receiving some flowers at her residence once and had asked Green about them. Green told J.U.F. not to throw the flowers away because they were sent to him from a friend for Green's birthday.

35. J.U.F. remembered receiving a package prior to Green's interview with the FBI on February 20, 2020. J.U.F. wanted to return the package to the sender because it was not addressed to J.U.F. or Green. However, Green said the package was for his friend. Green took the package, but J.U.F. did not know what the contents were or what Green did with it.

36. On September 16, 2020, affiant submitted multiple photographs of Lesley to the FBI FACE Services Unit for possible identification through facial recognition technology. On September 16, 17, and 21, 2020, affiant received responses from the FBI FACE Services Unit stating no candidates/matches were identified. Attempts to identify and confirm the existence of Lesley as a real person have met with negative results.

TECHNICAL INFORMATION REGARDING GOOGLE SERVICES

37. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

38. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

39. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device and a Google Account is required for certain functionalities on these devices.

40. Signing up for a Google Account automatically generates an email address at the domain “gmail.com”, like the email accounts listed in Attachment A. That email address will be the log-in username for access to the Google Account. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

41. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files on servers maintained and/or owned by Google.

42. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account

via Google's website or using a mobile application), details about the devices used to access the account and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

43. Google maintains the communications, files and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

44. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

45. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation. In addition, emails and attachments can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

46. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.*, information indicating a plan to commit a crime), or consciousness of guilt (*e.g.*, deleting account information in an effort to conceal evidence from law enforcement).

47. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation.

CONCLUSION

48. Based on the forgoing, I request that the Court issue the proposed search warrant.

49. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



PHILLIP W. SPAINHOUR
FEDERAL BUREAU OF INVESTIGATIONS

On this day, the applicant appeared before me by reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Subscribed and sworn to before me this 14th day of March 2022.



THE HONORABLE L. PATRICK AULD
UNITED STATES MAGISTRATE JUDGE